Written by **Selwyn Duke** on November 18, 2020

Engineer: Software-based Voting Must Die Before It Kills the Republic

Photo: cmannphoto / iStock / Getty Images Plus

Upon seeing election workers on TV poring over paper ballots and analyzing "hanging chads" during the contested 2000 election, many were aghast. "How could the United States use such 'backwards technology?!'" was the cry. But as people advocated electronic voting, I and others pointed out the obvious: Such technology allows the massive alteration of votes via software manipulation — perhaps by *just one person*. This is why, warns a top-notch computer engineer writing in 2020, for our Republic to live, software-based voting must die.

That man, Hank Wallace, has sterling credentials that include writing more than a million lines of code for major companies during the last 42 years and having been granted quite a few patents. Living and breathing his work, Wallace is a man who'll lie awake in bed at night designing systems and algorithms in his mind. It should thus give us pause when he says that putting his own ballot in an electronic voting machine sickens him because, he laments, he "cannot see what's behind the algorithmic curtain."

"You see, the great thing about software is that you can have a chunk of expensive electronic and mechanical hardware sitting there, and you can easily change the function of it with a simple software update," Wallace writes at *American Thinker*. This is great for software developers, he says, but disastrous when applied to systems critical to our Republic because they can be too easily corrupted.

The engineer then lists the ways cheating could be perpetrated, writing:

- Change the voting ratio between two candidates by any fraction
- Display an entered vote correctly to the voter, then change the vote before tabulation
- Display a summary of votes to an election official, and change that total later
- Allow remote modification of vote totals via the internet or local WiFi
- Change votes or methods at a certain time of day, or at a later date, even after voting machine certification concludes, or before/during auditing
- Change votes in a random fashion on election day [*sic*] to make it appear to be a legitimate voting trend
- Change voting trends by precinct, or using historical voting statistics
- Update the software secretly with a new algorithm

- Provide intermediate vote tallies to remote actors who are gaming the election in other ways
- Make adjustments to the votes of one candidate and tracking adjustments to other candidates down ballot

"Any cheat you could do with a paper ballot becomes extremely easy with an electronic voting machine, plus a lot more," Wallace then explains. "Want dead people to vote? You don't need to dig up their identification or voter registration card; just program the machine to register 1.02 Biden votes for every actual vote. So every 50 Biden votes result in one nonexistent person voting Biden as well. That's 2% that costs you no visits to the cemetery or morgue."

The issue lies not with the software or hardware, not with the design, Wallace correctly points out, but with the *designers*. Your election's integrity *can't be greater than theirs is*.

Artificial intelligence poses the same problem. It can be very convenient, but the reality is that many software engineers "grew up in amoral California or amoral socialist countries," notes Wallace, "and these people have zero moral inhibition writing A.I. code that conducts Big Tech criminal activity."

Realize also that it's not unusual for 90-plus percent of tech workers' donations to go to Democrats and that stories about the persecution of the rare conservative at Google or some other large tech company have made news in recent years. In other words, techies tend to have a definite political bias: They're notoriously left-wing.

The bottom line is that behind "every dishonest voting machine is a pile of dishonest programmers who have no moral inhibitions against giving local and regional politicians the tools they need to steal elections," writes Wallace. Pointing out that software geeks are a bit like idiot savants — skilled at their craft but ignorant in other areas — he warns that we shouldn't trust them with our futures and government. But right now that's *exactly what we're doing*.

There's yet another factor, however. Let's say you're a cracker-jack coder who can take his skills anywhere and who also has intense but twisted political passions. Might you not decide to work for a voting-machine company so that you can, aside from making great money, also indulge and effectuate those passions?

The point is that such people may be a minuscule percentage of programmers. But they exist and are *numerically* significant — and it only takes a few in the right positions to swing elections.

Speaking of which, there are allegations that electronic voting machines have already been used to swing elections in foreign countries and that Dominion machines, used in approximately 30 states, might have done so in our November 3 contest. In fact, it's also alleged that a man identified as Dominion's director of strategy and security, Eric Coomer, told Antifa members during a conference call that "Trump won't win. I made F***ing sure of that" (tweet below).

> Dominion Director of Strategy and Security, #EricCoomer:
>
> "Trump won't win. I made F***ing sure of that." https://t.co/brtQZi281D
>
> — Chanel Rion OAN (@ChanelRion) November 17, 2020

Whether or not this claim is accurate isn't really the point; the issue is that it *isn't far-fetched* — and that's a problem. This brings us to the claim that our recent election was fraud free.

To analogize this, it's as if we resolved to leave the doors and vaults of our banks open and the security cameras disabled every night and then said, "Don't worry, no one will steal anything! In fact, this is the safest banking situation in American history!"

Obviously, if a crime can easily be committed, it *will be committed* because a given trespass will always benefit a certain group of people. The above analogy is apt, too, and not just because of high-tech voting's outlined problems. Mail-in ballots, where the chain of custody is unknown and where, in certain cases, signature verification isn't even required, also present easy opportunities for fraudsters.

So how do you minimize vote fraud? Go *low* tech: paper ballots filled out in person with a pen on election day. The chain of custody must also be known, with ballots monitored by representatives of each major party and video surveillance. Counting them may be laborious, but making the process easy may equate to making vote fraud easy.

An impediment to this return to common sense is not just that fraud benefits a certain political party; it's also that the voting-machine business is lucrative and, I suspect, is donating money to politicians.

Whatever the case, the claim that our election was fraud-free is Orwellian. The truth is that, as in my banks analogy, our system lacks integrity. This guarantees vote fraud — the only thing in question then, ever and always, will be the degree.